

obligation to maintain effective controls against diversion. Failure to meet this obligation may result in remedial action consistent with §1301.36 of this chapter.

(e) An institutional practitioner that elects to conduct identity proofing must retain a record of the identity-proofing. An institutional practitioner that elects to issue the two-factor authentication credential must retain a record of the issuance of the credential.

**§ 1311.115 Additional requirements for two-factor authentication.**

(a) To sign a controlled substance prescription, the electronic prescription application must require the practitioner to authenticate to the application using an authentication protocol that uses two of the following three factors:

(1) Something only the practitioner knows, such as a password or response to a challenge question.

(2) Something the practitioner is, biometric data such as a fingerprint or iris scan.

(3) Something the practitioner has, a device (hard token) separate from the computer to which the practitioner is gaining access.

(b) If one factor is a hard token, it must be separate from the computer to which it is gaining access and must meet at least the criteria of FIPS 140-2 Security Level 1, as incorporated by reference in §1311.08, for cryptographic modules or one-time-password devices.

(c) If one factor is a biometric, the biometric subsystem must comply with the requirements of §1311.116.

**§ 1311.116 Additional requirements for biometrics.**

(a) If one of the factors used to authenticate to the electronic prescription application is a biometric as described in §1311.115, it must comply with the following requirements.

(b) The biometric subsystem must operate at a false match rate of 0.001 or lower.

(c) The biometric subsystem must use matching software that has demonstrated performance at the operating point corresponding with the false match rate described in paragraph (b) of this section, or a lower false match

rate. Testing to demonstrate performance must be conducted by the National Institute of Standards and Technology or another DEA-approved government or nongovernment laboratory. Such testing must comply with the requirements of paragraph (h) of this section.

(d) The biometric subsystem must conform to Personal Identity Verification authentication biometric acquisition specifications, pursuant to NIST SP 800-76-1 as incorporated by reference in §1311.08, if they exist for the biometric modality of choice.

(e) The biometric subsystem must either be co-located with a computer or PDA that the practitioner uses to issue electronic prescriptions for controlled substances, where the computer or PDA is located in a known, controlled location, or be built directly into the practitioner's computer or PDA that he uses to issue electronic prescriptions for controlled substances.

(f) The biometric subsystem must store device ID data at enrollment (*i.e.*, biometric registration) with the biometric data and verify the device ID at the time of authentication to the electronic prescription application.

(g) The biometric subsystem must protect the biometric data (raw data or templates), match results, and/or non-match results when authentication is not local. If sent over an open network, biometric data (raw data or templates), match results, and/or non-match results must be:

(1) Cryptographically source authenticated;

(2) Combined with a random challenge, a nonce, or a time stamp to prevent replay;

(3) Cryptographically protected for integrity and confidentiality; and

(4) Sent only to authorized systems.

(h) Testing of the biometric subsystem must have the following characteristics:

(1) The test is conducted by a laboratory that does not have an interest in the outcome (positive or negative) of performance of a submission or biometric.

(2) Test data are sequestered.

(3) Algorithms are provided to the testing laboratory (as opposed to scores or other information).